

CRYPTOLOGIA

Volume 32, Issue 1, 2008

Reading Encrypted Diplomatic Correspondence: An Undergraduate Research Project	1
<i>Jeffrey D. Adler, Ryan W. Fuoss, Michael J. Levin, and Amanda R. Youell</i>	
Improved Related-key Attacks on DESX and DESX+	13
<i>Raphael C.-W. Phan and Adi Shamir</i>	
Taking a Cryptology Class to Bletchley Park	23
<i>Chris Christensen and Suzanne Gladfelter</i>	
Key Enclosed: Examining the Evidence for the Missing Key Letter of the Beale Cipher	33
<i>Wayne S. Chan</i>	
Oblivious Transfer Based on Key Exchange	37
<i>Abhishek Parakh</i>	
Lessons Learned from a Mathematical Cryptology Course	45
<i>Brian Winkel</i>	
The Future of the Past—Questions in Cryptologic History	56
<i>David Kahn</i>	
Cicco Simonetta's Cipher-Breaking Rules	62
<i>Augusto Buonafalce</i>	
Breaking Short Playfair Ciphers with the Simulated Annealing Algorithm	71
<i>Michael J. Cowan</i>	
From the Archives: Intercepting Best Friend?	84
<i>Jan Bury</i>	
Review of The Collective Works of Captain George P. McGinnis by George P. McGinnis	88
<i>Chris Christensen</i>	
Review of How to Tell a Secret: Tips, Tricks & Techniques for Breaking Codes & Conveying Covert Information by P. J. Huff and J. G. Lewin . . .	90
<i>Chris Christensen</i>	
Review of Complexity and Cryptography: An Introduction by John Talbot and Dominic Welsh	92
<i>Joshua Holden</i>	
Review of Delusions of Intelligence by R. A. Ratcliff.	98
<i>John C. Gallehawk</i>	

Volume 32, Issue 2, 2008

Monument in Memoriam of Marian Rejewski, Jerzy Różycki and Henryk Zygalski Unveiled in Poznań	101
<i>Marek Grajek</i>	
Dilly Knox—A Reminiscence of this Pioneer Enigma Cryptanalyst	104
<i>Mavis Batey</i>	
Security Analysis of Authentication of Images Using Recursive Visual Cryptography	131
<i>Ching-Nung Yang and Tse-Shih Chen</i>	
Using Cartoons to Teach Internet Security	137
<i>Sukamol Srikwan and Markus Jakobsson</i>	
Structural Observations Regarding RongoRongo Tablet 'Keiti'	155
<i>Tomi S. Melka</i>	
From the Archives: Friedman Takes the Stand.	180
<i>David A. Hatch</i>	
Review of Figuring It Out At Bletchley Park 1939–1945 by John Gallehawk and Kerry Johnson	184
<i>Louis Kruh</i>	
Review of Voices of the Code Breakers: Personal Accounts of the Secret Heroes of World War II by Michael Paterson.	186
<i>Chris Christensen</i>	
Review of A^3 and His Algebra by Nancy E. Albert.	189
<i>Chris Christensen</i>	
Can You Break the NKU Monopoly?.	197

Volume 32, Issue 3, 2008

Captured Kriegsmarine Enigma Documents at Bletchley Park.	199
<i>Ralph Erskine</i>	
Algebraic Attacks on the Courtois Toy Cipher.	220
<i>Martin Albrecht</i>	
From the Archives: The Last Bombe Run, 1955	277
<i>Colin Burke</i>	
Review of Series on Arabic Origins of Cryptology	280
<i>James L. Massey</i>	
Review of <i>The History of Information Security: A Comprehensive Handbook</i> edited by Karl de Leeuw and Jan Bergstra	284
<i>Chris Christensen</i>	

Reviews of Cryptologic Fiction.	295
<i>John F. Dooley</i>	

Volume 32, Issue 4, 2008

How I Broke an Encrypted Diary from the War of 1812	299
<i>Kent D. Boklan</i>	
The 1942 Reorganization of the Government Code and Cypher School	311
<i>Christopher Grey and Andrew Sturdy</i>	
Breaking Short Vigenère Ciphers.	334
<i>Tobias Schrödel</i>	
Rejewski-Różycki-Zygalski Lectures in Computer Science	348
<i>Jerzy Jaworski</i>	
From the Archives: Inside a Cold War Crypto Cell. Polish Cipher Bureau in the 1980s	351
<i>Jan Bury</i>	
What Did We Do Before Biometric Passports? A Review of <i>Who Are You? Identification, Deception, and Surveillance</i> in Early Modern Europe by Valentin Groebner	368
<i>Whitfield Diffie</i>	

Following page 369:

Title Page for Volume 32
Table of Contents for Volume 32
Author Index for Volume 32

Author Index For Volume 32

- Adler, J. D., 1
Albrecht, M., 220

Batey, M., 104
Boklan, K. D., 299
Buonafalce, A., 62
Burke, C., 277
Bury, J., 84, 351

Chan, W. S., 33
Chen, T.-S., 131
Christensen, C., 23, 88, 90, 186, 189, 284
Cowan, M. J., 71

Diffie, W., 368
Dooley, J. F., 295

Erskine, R., 199

Fuoss, R. W., 1

Gallehawk, J. C., 98
Gladfelter, S., 23
Grajek, M., 101
Grey, C., 311

Hatch, D. A., 180
Holden, J., 92

Jakobsson, M., 137
Jaworski, J., 348

Kahn, D., 56
Kruh, L., 184

Levin, M. J., 1

Massey, J. L., 280
Melka, T. S., 155

Parakh, A., 37
Phan, R. C.-W., 13

Schrödel, T., 334
Shamir, A., 13
Srikwan, S., 137
Sturdy, A., 311

Winkel, B., 45

Yang, C.-N., 131
Youell, A. R., 1

